



BULLETIN DE SECURITE

Titre	Vulnérabilités critiques dans Google Android and Pixel
Numéro de Référence	49140409/24
Date de Publication	04 septembre 2024
Risque	Critique
Impact	Critique

Systemes affectés

- Google Android versions 11, 12, 12L, 13, 14 sans le correctif de sécurité du 3 septembre 2024

Identificateurs externes

- CVE-2024-23358 CVE-2024-23359 CVE-2024-23362 CVE-2024-23364 CVE-2024-23365
CVE-2024-23716 CVE-2024-29779 CVE-2024-31336 CVE-2024-32896 CVE-2024-33016
CVE-2024-33034 CVE-2024-33035 CVE-2024-33038 CVE-2024-33042 CVE-2024-33043
CVE-2024-33045 CVE-2024-33048 CVE-2024-33050 CVE-2024-33051 CVE-2024-33052
CVE-2024-33054 CVE-2024-33057 CVE-2024-33060 CVE-2024-3655 CVE-2024-36972
CVE-2024-39431 CVE-2024-39432 CVE-2024-40650 CVE-2024-40652 CVE-2024-40654
CVE-2024-40655 CVE-2024-40656 CVE-2024-40657 CVE-2024-40658 CVE-2024-40659
CVE-2024-40662 CVE-2024-44092 CVE-2024-44093 CVE-2024-44094 CVE-2024-44095
CVE-2024-44096

Bilan de la vulnérabilité

Google a publié des mises à jour de sécurité pour corriger plusieurs vulnérabilités affectant les appareils Android. L'exploitation réussie de ces vulnérabilités peut permettre à un attaquant non authentifié de causer un déni de service sur des appareils Android vulnérables, de porter atteinte à la confidentialité des données ou de réussir une élévation de privilèges.

Solution

Veuillez se référer au bulletin de sécurité Google Android du 03 septembre 2024 afin d'installer les nouvelles mises à jour.

Risque

- Atteinte à la confidentialité des données,
- Élévation de privilèges,
- Dénier de service

Référence

Bulletin de sécurité Android du 03 septembre 2024:

- <https://source.android.com/docs/security/bulletin/2024-09-01?hl=fr>
- <https://source.android.com/docs/security/bulletin/pixel/2024-09-01?hl=fr>